



Mission Success Starts With Safety ²

Introduction

- Welcome!
- Points of Contact:
 - Cal Staibus, NASA KSC - Tel: (321) 867-8757; calvert.a.staibus@nasa.gov
 - Shawn Donovan, SRS Technologies - Tel: (321) 867-6240; shawn.t.donovan@nasa.gov



OSTM



Mission Success Starts With Safety ³

Topics

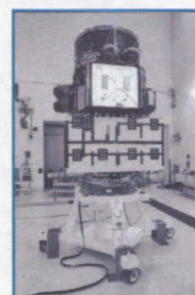
- Background
 - Current NASA ELV Payload Safety Review Process Standard
- Format of NPR 8715.XX
 - Chapter 1: Introduction, Payload Safety Policy, Programmatic Roles and Responsibilities, Tailoring and Waiver Processes
 - Chapter 2: Introduction, Payload Safety Working Group, Project Roles and Responsibilities, Flow of Activities and Deliverables, Content of Deliverables, & Data Submittals



Mission Success Starts With Safety ⁴

Background

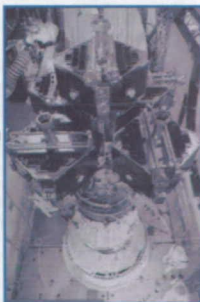
- NASA STD-8719.8, "ELV Payload Safety Review Process Standard"
 - Applies to Orbital and Deep Space ELV Missions (unmanned)
 - Focus on safety of processing at launch site, including payload processing facilities at or near launch site
 - Designed for missions involving numerous organizations and various vehicle/launch site combinations



Mission Success Starts With Safety ⁵

Background (continued)

- NASA STD-8719.8 (continued)
 - Has been successful (with ad hoc changes) for a majority of NASA ELV payloads
 - Certain complications evolved after the Process was developed:
 - Complicated roles for projects involving multiple NASA Centers
 - Projects involving International Partners
 - Lack of approval process for use of common spacecraft bus
 - Lack of process for resolving dissenting opinions within NASA and with external organizations
 - Lack of acceptance of external approving authority and requirements



Mission Success Starts With Safety ⁶

Cloud-Aerosol LIDAR and Infrared Pathfinder Satellite Observation (CALIPSO) Spacecraft

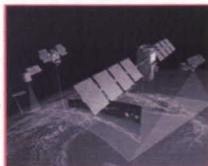
Highlighted weaknesses in current payload safety review process

- Launched from VAFB SLC2, April 2006
- Co-manifested with CLOUDSAT - Led by Goddard
- NASA provided CALIPSO instrument - France provided spacecraft bus
 - "Off the shelf" hydrazine-fueled Proteus spacecraft manufactured by Alcatel Space Industries and provided by the Centre National d'Etudes Spatiales (CNES) as its "contribution" to the joint mission
 - Joint Mission Agreement - not your typical contract
- Proteus flown successfully in 2001 on the Jason-1 - led by JPL
- Goddard SMA and Engineering raised concerns with Proteus:
 - Fault tolerance for leakage of hydrazine, software safety, battery safety, others
- Resolution via Formal Variance Process:
 - Personnel safety ensured via implementation of NESC recommendations
 - Mission success risk accepted via NASA Variance



**Background (continued)**

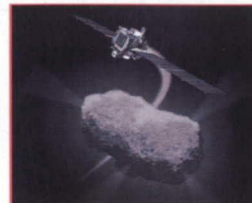
- Current process requires a Payload Safety Working Group (PSWG) for each payload with representatives from all involved organizations:
 - PSWG membership by a Center/organization sometimes varies for the same mission, and from one mission to the next (even when a common, previously approved spacecraft bus is assessed)
 - Lack of communication between members within some organizations
 - Technical concerns sometimes handled differently for similar payloads (not necessarily a problem, but can be)



CLOUDSAT/CALYPSO

**Background (continued)**

- Relies heavily on other agencies' requirements (e.g., Air Force)
 - Subject to other agencies' interpretation of requirements
 - Other agencies' safety focus perceived to vary when it is not their payload
 - NASA's authority is sometimes misunderstood and decisions challenged when using other agencies' requirements documents



DEEP SPACE 1

**Background (continued)**

- Requires "Tailoring" of requirements for each payload
 - Subject to misunderstanding the process and poor implementation
 - Current Process lacks the strict and consistent oversight from one project to the next needed for proper implementation
- Relies heavily on the ability of the PSWG to reach consensus
 - No identification of a decision-making authority
 - No clear direction for when consensus cannot be reached
 - Resolution of contentious issues can drag-on until the "final hour"
 - No clear direction on the applicable Safety Waiver Process



GENESIS

**Background (continued)**

- Issues addressed by this program:
 - Complicated roles and responsibilities associated with multi-partner projects
 - Working relationships and communications between all organizations involved in the payload safety process
 - Consistent interpretation and implementation of safety requirements from one project to the next
 - Consistent implementation of the Tailoring Process
 - Clearly defined NASA decision-making authority
 - Bring Agency-wide perspective to each ELV payload project



EUROPA Explorer

**Program Development**

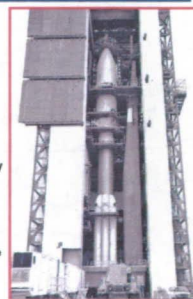
Agency Team Established by Bryan O'Connor and managed out of KSC by Cal Staibus as the ELV Payload Safety Program Manager

KSC	Cal Staibus
GSFC	Bo Lewis, Jamie Harper
JPL	Jim Lumdsen, Ben Lucas
HQ	Mike Dook

- Develop Program guidance as needed
- Resolve Working Group comments
 - Strive to build consensus on Program Elements
 - Chief OSMA has final decision making authority
- Ensure Program is consistent with current Agency implementation of Technical Authority
- Coordinate with external organizations

**Program Development (continued)**

- Build on the PSWG approach and augment as needed with lessons learned
- New Agency Safety Program to Include:
 - Establish and maintain NASA ELV Payload Safety Policy, Roles and Responsibilities, and Associated Requirements
 - Ensure consistent interpretation of safety requirements
 - Define and oversee implementation of the safety review process
 - Provide payload projects with training, tools, and guidance
 - Identify Decision Making Authorities
 - Formal process for resolving differences within the PSWGs
 - Formal tailoring and waiver processes
 - Enhance and formalize key partnerships (e.g., Air Force, commercial launch services, etc.)



NEW HORIZONS on an ATLAS V

**NPR 8715.XX Format**

- Chapter 1:
 - Introduction
 - Payload Safety Policy
 - Programmatic Roles and Responsibilities
 - Tailoring and Waiver Processes
- Chapter 2:
 - Payload Safety Working Group
 - Project Roles and Responsibilities
 - Flow of Activities and Deliverables
 - Content of Deliverables
 - Data Submittals

**Applicability****NPR 8715.XX Applies to:**

- Unmanned orbital and unmanned deep space payloads managed or launched by NASA whether developed by NASA or any contractor or independent agency in a joint venture with NASA
- ELV payload contracts, design, fabrication, testing, vehicle integration, launch processing, launch, and planned recovery of ELV payloads; payload provided upper stages flown on ELVs; interface hardware that is flown as part of a payload; and GSE used to support payload related operations

**Applicability (cont.)**

- NPR 8715.XX Does not Apply to:
 - Payloads that interface with a manned launch vehicle or spacecraft
 - Payloads that will fly on suborbital launch vehicles
 - Non-NASA payloads launched from Wallops Flight Facility where NASA is just providing range services

**Applicability for Existing Projects**

- The project must coordinate with the PSWG and ELV Payload Safety Manager for applicability of the NPR to the remainder of the project
- The level of implementation will vary based upon:
 - the project's success in complying with applicable technical safety requirements
 - the level of inherent safety risk
 - the completion of project safety milestones
- Existing safety-related approvals and decisions will be honored unless a new safety issue warrants further assessment and approval



DEEP IMPACT

**NASA ELV Payload Safety Policy**

- Safeguard people and resources (including flight hardware and facilities) from hazards associated with ELV payloads, integration, and payload related GSE by eliminating the hazards or reducing the risk to an acceptable level. Accomplished by:
 - Establishment and maintenance of technical and procedural safety requirements applicable to design, production, prelaunch processing and testing, vehicle integration, launch, and planned recovery payloads
 - Coordination with U.S. or foreign entities as needed to identify and ensure compliance with agreed to safety requirements

**NASA ELV Payload Safety Policy (continued)**

- Incorporation of safety requirements into the overall requirements for each payload, the contracts for related procurements, and cooperative or grant agreements
 - *It is the intent of this program to ensure adherence to applicable safety requirements that provide an equivalent level of safety for all NASA ELV payloads, other resources, and personnel regardless of where the payload is being processed*
- An independent payload safety review and approval process designed to ensure that each project implements all applicable safety requirements and facilitates safety risk management



THEMIS Launch

**ELV Payload Safety Agency Team**

An element of OSMA that functions to provide Agency-wide perspective and insight in support of the SMA Technical Authority

- Independently assess projects to assure that policy and requirements of this program are consistently implemented throughout the Agency
- Assure identification of safety concerns for each project and any applicability to other payloads
- Coordinate any safety concerns with the project's PSWG as early as possible
- Provide guidance to the Chief, Safety and Mission Assurance, and the SMA Technical Authorities, including issues requiring an Agency-level decision

**ELV Payload Safety Agency Team (cont)**

- Assure consistent interpretation of requirements and provide guidance on implementation
- Issue interim guidance as needed
- Provide the SMA Technical Authorities with assessments of alternative approaches proposed as part of the Tailoring and Waiver processes
- Ensure that any mission specific decision made by the Agency Team is consistent with the safety requirements of other organizations that share safety responsibility for the mission



STARDUST

**Center Director responsible for a Payload, Payload Processing Facility, or Launch Site**

- Establish the Center-level processes and associated requirements needed to implement the policy of this program
- Support safety assessments and respond to findings and recommendations
- Ensure that applicable personnel complete training on the NASA ELV payload safety requirements, safety review and approval process, and related activities
- Ensure that Center institutional resources provided to support activities comply with applicable technical and procedural requirements



MARS GLOBAL SURVEYOR

**Center SMA Director responsible for a Payload, Payload Processing Facility, or Launch Site**

- Ensure implementation of this program for each project that uses the Center's resources
- Provide each project with safety engineering, safety analysis, and other safety expertise needed to ensure the project successfully completes the safety review and approval process
- Ensure that processes exist and assessments are conducted to ensure compliance with this program and the safety of activities within the scope of their authority



Phoenix Mars Rover

**ELV Payload Project Manager**

- Ensure resources are allocated to satisfy all aspects this program
- Ensure that the project technical development, design, test and review processes incorporate system safety engineering
- Ensure that the design and operations of flight hardware, software, and associated GSE provides for safety through the use of approved design, analysis, and verification techniques
- Ensure the project's timeline complies with the established review and approval process
- Establish and implement any project-level processes and requirements needed to satisfy safety requirements and complete safety review and approval process

**ELV Payload Project Manager (cont.)**

- Ensure that the project's tailored requirements document is implemented for its payload and associated GSE or a waiver is obtained
- Ensure spacecraft contractor oversight is defined, performed, and documented to enable safe integration, testing, and processing of the payload and prevention the transfer of unanticipated hazards
- For an existing project, coordinate with the PSWG and Agency Team to determine the applicability of this program to the remaining phases of the project



NASA Contract, Grant, Cooperative Agreement, or Other Agreement Officers

- Ensure that all applicable safety and mission assurance requirements are incorporated into the contracts and agreement(s) governing each payload, including compliance with this NPR 8715.XX, NPR 8715.3, NPD 8730.2, Federal, State, and local requirements and compliance with and using NPR 5800.1, Grant and Cooperative Agreement Handbook for grants



CALYPSO



Tailoring Process

- The Payload Project Office is responsible for the tailored requirements document to be completed and approved in accordance with NPR 8715.xx
- After approval, any further changes to the tailored requirements document must be documented and distributed as a "change page" by the Payload Project Office for coordination and approval/concurrence by the original authorities
- If the tailoring of a requirement (i.e., deletion of a requirement, a change to a requirement, or an approach that differs from the stated requirement) results in a increased safety risk, the Payload Project Office shall prepare a waiver request
 - *Note: An approach that differs from the stated requirement may be approved as part of the tailored requirements document provided it does not result in increased safety risk and the document contains sufficient rationale.*
- In the event that an authority does not concur on a tailored requirements document and the issue cannot be resolved through coordination with the PSWG, the Agency Team, or the SMA Technical Authority(ies), all interested parties shall brief their position to the Chief, Safety and Mission Assurance to identify the best approach to achieve resolution



Tailoring Process

- The overall intent of the ELV payload safety requirements tailoring process is to ensure appropriate oversight of Agency requirements while providing the Centers and project managers with the authority and flexibility needed to accomplish their tasks. Tailoring is defined as the process of assessing the applicability of requirements and evaluating the potential compliance by a project in order to generate a set of specific requirements for that project.
- The Payload Project Office and the payload project system safety engineer shall work with the PSWG to identify applicable requirements and to tailor a set of mission specific safety requirements that are compiled into a mission specific document
- The PSWG Chairperson and Agency Team shall coordinate to ensure consistent application of tailoring throughout the Agency. The PSWG Chairperson and the ELV Payload Safety Manager shall coordinate to ensure that authorities involved in the mission or having responsibility for issues addressed by the tailoring, approve (sign) each tailored requirements document or provide equivalent written approval
- The signatories of each tailored requirements document shall include, but are not limited to the Payload Project Manager and responsible NASA Technical Authority(ies) (SMA, Engineering, and Health and Medical as applicable)



Waiver Process

- For the NASA ELV Payload Safety Program, a waiver is defined as a written authorization granting relief from a requirement and documenting the acceptance of any associated safety risk.
- Each Payload Project Manager or designee shall coordinate with their mission PSWG as soon as the project identifies a potential non-compliance with a safety requirement
- The Payload Project Manager or designee shall draft the waiver request



Waiver Process

- The Payload Project Manager or designee shall coordinate each waiver request with the PSWG and the Agency Team to:
 - Ensure the waiver request and accompanying data are correct and complete
 - Ensure any risk is properly characterized and that any increase in overall risk is identified
 - Assess any effects the waiver might have on other projects, resources or requirements
 - Ensure appropriate signatures for approval, concurrence, and risk acceptance per the requirements of NPR 8715.3



NEW HORIZONS



Waiver Process

- In addition to satisfying the requirements of NPR 8715.3, the signatories of each waiver shall include:
 - The Payload Project Manager
 - Responsible NASA Technical Authority(ies) (SMA, Engineering, and Health and Medical as applicable),
 - All other authorities involved in the mission or having responsibility for issues addressed by the waiver
- The ELV Payload Safety Manager shall coordinate with the Agency Team and each PSWG Chairperson to ensure a consistent waiver approach for all NASA ELV Payloads
- In the event that a required signatory does not concur or approve a waiver and the issue cannot be resolved through coordination with the PSWG, the Agency Team, or the SMA Technical Authority(ies), all interested parties shall brief their position to the Chief, Safety and Mission Assurance to identify the best approach to achieve resolution



Project Roles and Responsibilities



Huygens Probe and Titan

Image Credit: Craig Atchberry



Each ELV Payload Project Manager

- Ensure that a Payload Organization Safety Engineer is appointed
- Ensure the Payload Safety Introduction Briefing is coordinated and scheduled early in Phase B as defined in NPR 7120.5
- Notify the NASA ELV Payload Safety Manager of the new project and provide contact information for the appointed Payload Organization Safety Engineer
- Coordinate with the NASA ELV Payload Safety Manager to ensure that the project's PSWG is established and functions as required by this NPR



THEMS at ARTNOTCH



Each ELV Payload Project Manager

- Coordinate with the NASA ELV Payload Safety Manager to ensure that the PSWG includes the following members, as applicable, to each mission:
 - (1) NASA Payload Organization Safety Engineer
 - (2) Payload contractor safety representative(s)
 - (3) Launch site range safety organization representative(s)
 - (4) Launch vehicle contractor safety engineer
 - (5) Payload processing facility safety representative
 - (6) NASA Launch Services Division Safety Engineer
 - (7) PSWG Chairperson
- Note: Typically, the NASA Launch Services Division Safety Engineer also serves as the PSWG Chairperson. Depending on the mission specifics, there may be advantages to having a PSWG representative from one of the other NASA organizations involved in the mission perform this function. A Co-Chairperson may also be appointed if deemed necessary for any mission.
- Composition of the PSWG and member participation may vary based on project activities, technical issues, multi-Center project involvement, or operational requirements (for example, selection of launch vehicle or processing facility; end-of-mission sample recovery activities).



Payload Safety Working Group Membership



*Invited participant

Note: NASA Launch site safety organization will most likely chair



Each ELV Payload Project Manager

- Ensure all project personnel involved in the ELV payload safety review process receive training on the process, understand their associated roles and responsibilities, and have experience commensurate with the complexity of the project
- Ensure that the project plans, fully participates, and supports the safety review and approval process activities of NPR 8715.XX
- Ensure the safety status and any safety concerns associated with each subsystem and integrated system are presented at appropriate project reviews, including (but not limited to) System Requirement Reviews, Preliminary Design Reviews, Critical Design Reviews, Pre-Environmental Reviews, and Pre-Ship Reviews
- Approve all safety review and approval process deliverables of this NPR prior to submittal to the PSWG



Each ELV Payload Project Manager

- Obtain all safety approvals and safety readiness products needed to accomplish project management requirements per NPR 7120.5 and accomplish mission processing. These shall include:
 - Notification from the PSWG Chairperson of acceptable Safety Review I deliverables and satisfactory completion of Safety Review I
 - Note: Successful completion of Safety Review I and associated deliverables is a safety readiness gate product required prior to the project's Key Decision Point C.
 - Notification from the PSWG Chairperson of acceptable Safety Review II deliverables and satisfactory completion of Safety Review II
 - Note: Successful completion of Safety Review II and associated deliverables is a safety readiness gate product required prior to the project's Key Decision Point D.
 - Notification from the NASA ELV Payload Safety Manager indicating that the project has successfully completed Safety Review III and is ready to proceed with shipping and commence prelaunch processing

**Each ELV Payload Project Manager**

- Ensure that the project fully implements all safety plans and procedures required by this NPR
- Ensure that the status of any open items in the Safety Action Tracking Log or any payload safety issues that could impact launch schedule are briefed during safety and project reviews
- Ensure that the PSWG Chairperson is notified of any mishaps or close calls that take place during launch area payload processing and ground operations

**Agency Team**

- The Agency Team shall assist each PSWG, as needed, to resolve any conflicts regarding compliance with this NPR
- The Agency Team shall coordinate to provide a single position on any guidance or comments provided to a PSWG. This includes interpretation of requirements and approval of alternative approaches to satisfying safety requirements.
- The Agency Team shall perform independent assessment to ensure compliance with Agency objectives and requirements identified by this NPR

**The Payload Organization Safety Engineer**

- Perform as the payload organization's primary member of the PSWG
- Ensure the preparation and submittal of all safety review and approval process deliverables in accordance with schedule timeline requirements and following the format and content requirements specified in NPR 8715.xx
- Ensure the implementation of all safety related plans and activities approved by the PSWG
- Ensure that the payload design process incorporates system safety engineering activities integral to identifying hazards, developing solutions to mitigate or eliminate the hazards, verifying the implementation of these solutions, and ensuring compliance with this NPR
- Keep the Payload Project Manager informed of mission safety status

**The Payload Organization Safety Engineer**

- Ensure that a Safety Verification Tracking Log (SVTL) is established, maintained and made available for viewing electronically by the project, PSWG and Agency Team to track closure of each open hazard control verification identified in the hazard reports. SVTL status shall be presented at the Safety Review III
- Ensure that a Safety Action Tracking Log is established and maintained for the project to track closure of safety actions
- Ensure that technical operating procedures are submitted for review and approval by safety and other responsible organizations, in accordance with the safety requirements of the specific operating location
- Present mission safety information at appropriate project reviews as required by NPR 7123.1 and this NPR
- In coordination with the PSWG Chairperson, establish and maintain an integrated schedule of PSWG activities and all relevant project, launch, and other mission milestones, reviews, or meetings that address the topic of payload safety to include place, time, and date for each activity

**Each PSWG member**

- Participate in the safety review and approval process
- Ensure compliance with all safety requirements for their area of responsibility and authority
- Review and provide comments to the project on all payload safety review deliverables and meeting minutes within 30 days after submittal
- Assess and concur (or obtain concurrence from their management as needed) on tailoring and any waiver to a safety requirement that is within their scope of responsibility
- Coordinate with the PSWG to resolve payload safety concerns and if needed, with the Agency Team
- Ensure that payload, facility, and payload/launch vehicle integration issues are disseminated to their organization and to other PSWG members

**Each PSWG member**

- Participate in all PSWG activities associated with their areas of responsibility, including but not limited to meetings, mission safety reviews, design reviews, ground operations reviews, and others activities as required by the PSWG Chairperson
- Assess and concur on plans and hazard reports for operations in facilities that fall under their safety responsibility as needed to receive and process the payload



AURORA Imaging



The PSWG Chairperson

- Schedule and conduct PSWG meetings
- Ensure that PSWG activities and decisions include input and participation all its members
- Provide official PSWG signature (indicating concurrence from all PSWG members) for all deliverables and correspondence
- Ensure deliverables are available
- Ensure that the PSWG and Agency Team are invited to PSWG activities
- Ensure all comments to deliverables are organized and submitted to the project ≤35 days after submittal



The PSWG Chairperson

- Ensure PSWG activities are documented - e.g. notices, scheduling, action items, key issues, decisions and status of the safety review and approval process
- Ensure distribution of final minutes
- Ensure appropriate notification of the project safety schedule and changes
- Ensure PSWG participation by appropriate PSWG members at payload/launch vehicle integration working group meetings
- Schedule and conduct PSWG meetings concurrently with major project reviews and as required to meet the safety milestones of this program



The PSWG Chairperson (cont.)

- Ensure the Agency Team is informed of important safety issues, e.g. potential risk issues, that may impede the safety review process
- Ensure that all mission support and safety related documents are filed for access on a secure website by the PSWG members, Agency Team, the NASA ELV Payload Safety Manager or other subject matter experts or technical authorities
- If the PSWG cannot reach consensus on an issue, the PSWG Chairperson shall coordinate with the NASA ELV Payload Safety Manager to establish a resolution approach
- Coordinate with the PSWG and the project to ensure implementation of recommendations, interpretations, and resolutions of any safety concern provided by the Agency Team



The NASA Launch Services Program Manager

- Provide the funding and other resources needed to ensure that personnel from the launch vehicle contractor (once under contract), Launch Services SMA, and the Range participate in the safety review process beginning no later than the Payload Safety Introduction Briefing
- Notify the PSWG of program integration meetings including Ground Operations Working Group, Ground Operations Review, Mission Integration Working Group, and others
- Ensure that the NASA Launch Services Division Safety Representative is notified of any payload/launch vehicle interface safety concerns
- Ensure launch services contracts for launch vehicle and commercial payload processing facility contracts contain the provisions needed to satisfy the requirements of this NPR (including requirements incorporated by reference)

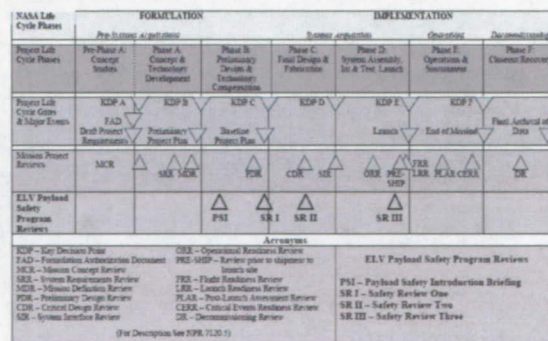


The NASA ELV Payload Safety Manager

- Track the status of each payload project as it proceeds through the safety review and approval process and provide guidance on the associated activities, tools, and deliverables as needed
- Shall notify the Payload Project Manager and other authorities:
 - If a major safety related risk that may adversely impact the project is identified any time during this safety review process
 - If the required safety review activities or deliverables of this NPR are not met (or product quality is inadequate for that phase of the project lifecycle) and fail to fulfill the required safety gate products prior to the project's Key Decision Points per NPR 7120.5 and provide guidance on how the project should proceed
- Sign the Certificate of Safety Compliance upon ensuring that all Agency Team concerns are resolved
- Issue a letter forwarding the Certificate of Safety Compliance to the Payload Project Manager and others signifying the successful completion of the ELV Payload Safety Review III and readiness to proceed with shipping and processing



Timeline of ELV Payload Safety Reviews





Flow of Activities and Deliverables

- The Payload Organization Safety Engineer ensures the preparation and submittal of the associated deliverables for review.
 - *Note: The safety review and approval activities are designed to coincide with the project management reviews required by NPR 7120.5, e.g., Preliminary Design Review, Critical Design Review, and Pre-ship Review. The safety review and approval activities identified below are not inclusive of other required project, NASA HQ, or Center S&MA reviews which should include Peer Reviews, Launch Readiness, Facility S&MA readiness, etc.*
- The payload project and the PSWG shall ensure that the safety review and approval process incorporates the following sequence of activities and associated deliverables including compliance with the associated required schedule timing of deliverables
- *Exception: Process and deliverable dates required by NPR 8715.XX may be altered through advanced formal agreement between the Payload Project Office and the PSWG provided that safe processing, project schedule, and safety review input to Key Decision Points as defined in NPR 7120.5 are not impacted.*



A Payload Safety Introduction Briefing

- Shall occur as early as possible but no later than midpoint of the Preliminary Design Phase (Phase B as defined in NPR 7120.5). This should be the first meeting of the PSWG. The payload project shall submit:
 - As a precursor to the tailoring processes, identification of the safety requirement documents that are applicable to the project; applicable previously approved waivers and alternative approaches, and known tailoring issues for presentation and review during the Payload Safety Introduction Briefing
 - Draft Systems Safety Plan that, as a minimum, provides a conceptual overview of the Systems Safety Program, for presentation and review at the Payload Safety Introduction Briefing
 - Identification of known spacecraft/payload systems and a preliminary assessment of potential hazards documented in a preliminary hazard list for presentation at the Payload Safety Introduction Briefing
 - A basic Ground Operations Flow Overview providing the location and timeline of major payload activities and tasks for presentation at the Payload Safety Introduction Briefing
- *Note: This briefing provides a forum for the project to introduce the mission to the PSWG and other authorities and allows for early identification of any safety concerns associated with the payload. The information provided at this briefing should be as complete as the technical maturity of the conceptual design and operations allow.*



Safety Review I

- Begins with the submittal of data prior to the PDR and shall be completed ≤60 days after the project's PDR or no later than necessary to provide the PSWG's input to the project's Key Decision Point C as defined in NPR 7120.5, whichever date comes first
 - Safety Review I shall include a PSWG meeting held in conjunction with the PDR
 - During Safety Review I the PSWG shall approve the final System Safety Plan, discuss the resolution of comments to the Safety Data package, address requirements issues through the review of the tailored requirements, assess the Preliminary Hazard Analysis and any Hazard Reports, and address any safety issues identified during the Preliminary Design Review
 - The payload project shall submit:
 - Final System Safety Plan ≤30 days prior to the PDR meeting
 - Tailored Payload Safety Requirements ≤30 days prior to the PDR meeting
 - Safety Data Package I (as complete as possible) ≤30 days prior to the PDR



Safety Review I (cont.)

- The PSWG Chairperson shall provide the Payload Project Manager with the status of Safety Review I including any safety concerns following the Preliminary Design Review meeting
- Safety Review I shall culminate with the PSWG Chairperson providing the Payload Project Manager with an assessment of the project's safety efforts and identification of any safety concerns to support the project's Key Decision Point C (as defined in NPR 7120.5)



TOPEX/Poseidon



Safety Review II

- Begins with the submittal of data prior to the project's CDR and shall be completed ≤60 days after the project's CDR to provide the PSWG's input to the project's Key Decision Point D as defined in NPR 7120.5
 - Safety Review II shall include a PSWG meeting held in conjunction with the CDR
 - During the Safety Review II, the PSWG shall discuss the resolution of comments to the Safety Data Package I, discuss any safety issues identified during the CDR, and review the project for any changes to the design, processing, or interfaces for new or increased hazards or safety issues
 - The payload project shall submit:
 - Safety Data Package II ≤30 days prior to the Safety Review II meeting
 - Final Tailored Payload Safety Requirements ≤30 days prior to the Safety Review II meeting
 - The project Safety Action Tracking Log, for concurrence to close completed actions, and review of open actions and status



Safety Review II

- Safety Review II shall culminate with the PSWG Chairperson providing the Payload Project Manager with an updated assessment of the project's safety efforts and identification of any safety concerns to support the project's Key Decision Point D (as defined in NPR 7120.5)
- If the payload will undergo processing at a NASA-owned facility or any facility where NASA personnel control the operation or are actively involved in performing work prior to the Safety Review III, the project shall coordinate to define the applicable requirements and processes for safe payload processing at the host center that meet the intent of the requirements defined in this NPR



Safety Review III

- Begins with the submittal of data and shall be completed at a PSWG meeting at least 30 days prior to the project's Pre-ship Review
- During Safety Review III the PSWG shall verify that all safety requirements have been satisfied or any associated waivers have been approved
- The payload project shall submit:
 - A Safety Data Package III ≤60 days prior to the Safety Review III and shall be finalized satisfying all comments at least 30 days before the intended shipment of hardware to the prelaunch payload processing site
 - A Safety Verification Tracking Log identifying the open verifications from the Hazard Reports
 - A Safety Action Tracking Log current to the Safety Review III meeting, for concurrence to close completed actions, and review of open actions and status



Safety Review III

- The project shall provide a Certificate of ELV Payload Safety Compliance signed by the Project Manager and with signature blocks for the PSWG Chairperson and the ELV Payload Safety Manager
- Safety Review III shall culminate with the PSWG Chairperson and the ELV Payload Safety Manager signing the Certificate of ELV Payload Safety Compliance indicating that the project has safety approval to ship the payload to the launch area

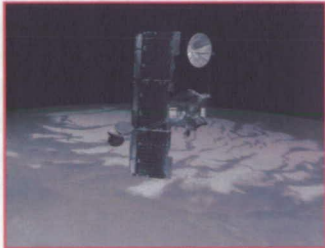


DEEP SPACE



Certificate of ELV Payload Safety Compliance

- The ELV Payload Safety Manager shall provide the Payload Project Manager with a letter (or equivalent) within 5 days of successful completion of Safety Review III with copies to other officials as appropriate for each mission.



ODYSSEY over mars south pole



Certificate of ELV Payload Safety Compliance

- The letter shall:
 - Indicate that the project has successfully completed the payload safety review process per this NPR
 - Include a copy of the signed Certificate of ELV Payload Safety Compliance including any addendum
 - Identify all conditions or constraints applicable to the safety approvals



Once the payload is shipped

- After transportation of the payload to the launch area processing facility, the project shall update the Safety Verification Tracking Log at least weekly (more frequently if the open items must be closed to remove operational constraints) and make the current Safety Verification Tracking Log available to all officials involved in the mission.



LUNAR Prospector



Content of Deliverables



Content of Deliverables

- The payload project in coordination with the PSWG shall:

- Ensure that the content of the deliverables satisfies the requirements of NPR 8715.XX
- Ensure that the level of technical detail is commensurate with the project's life cycle phase
- Ensure that changes are annotated for easy location and verification



AIM fully deployed



Tailored Payload Safety Requirements

- Document all safety requirements that apply to a payload mission
- Use AFSPCMAN 91-710 as the baseline document for tailoring and include any applicable NASA and local safety requirements that are in addition to those in AFSPCMAN 91-710
- In the event of conflicting requirements, incorporate the more stringent
 - *Note: A majority of safety requirements applicable to NASA ELV payloads are currently documented in the Air Force requirements document, AFSPCMAN 91-710. The NASA ELV Payload Safety Program is in the process of developing a new NASA Standard that will be a compilation of NASA and Air Force requirements as tailored for NASA ELV payload missions and augmented with implementation guidance for NASA ELV payload projects where appropriate. The new NASA Standard will provide a single baseline requirements document that each payload project will tailor for approval by NASA, the Air Force, and other approving authorities. When the new NASA Standard is completed, this NPR will be revised to reference the new NASA Standard.*
 - In addition, local safety requirements must be met for all areas where the payload is processed, transported, integrated, and launched. The responsible PSWG members will assist in identifying applicable local safety requirements.



Tailored Payload Safety Requirements

- Document the applicability of safety requirements to specific situations within a mission
- Document the interpretation of requirements as needed
- Address any recommendations, interpretations, or resolutions of safety concerns provided by the Agency Team and each authority involved in the mission
- Identify any change to a requirement (i.e., any addition or deletion from the source requirement) and include sufficient rationale for the tailored change
- Identify potential areas of non-compliance with applicable requirements
- Reference any waivers identified during the tailoring process



A Payload Safety Introduction Briefing

- shall provide the following information to a level of detail consistent with the complexity of the mission, the maturity of the conceptual design, and determination of the launch vehicle and launch site location:
- Overview of the System Safety Program as defined by the project's System Safety Plan
- Identification of organizational roles and responsibilities
- Identification of applicable safety requirements and compliance documents
- Description of payload, instruments, and anticipated ground support equipment
- Description of the flight path in terms of azimuth and trajectory, identification and description of planned recovery activities and support for sample/payload return if applicable
- Identification of potential payload/launch vehicle interfaces, and mission unique ground support equipment required for pad operations
- Identification and a preliminary assessment of potential hazards associated with payload to launch vehicle integration, multiple payloads, and ground systems documented in a preliminary hazard list



A Payload Safety Introduction Briefing

- Overview of Draft Requirements Tailoring, identifying critical assumptions to be made during the tailoring process
- Identification of any potential non-compliances to NASA, NASA Center, commercial processing facility, Air Force Range, or Federal Requirements
- Any potential hazardous failure modes, failure probability, and performance characteristics of the payload during ground operations
- Identification of planned studies and analyses that support safety requirements, including scheduled completion
- Description of processing flow and anticipated schedule, integrated with major project milestones
- Identification of facility requirements, including launch complex, hazardous assembly and checkout areas, and ordnance and propellant storage requirements
- Identification and discussion of potential contingency operations, for example, depressurization, propellant offload, and accessibility after fairing installation
- Overview of the Mishap Preparedness and Contingency Plan(s) and their approach for communicating, documenting, and investigating payload pre-launch contingencies including close calls, lessons learned, and mishaps, potential project specific emergency response; and anticipated data impound responsibilities as required by NPR 8621.1
- Recommendations for future safety Technical Interchange Meetings, reviews, working groups, subject matter expert support, resolution of unmet requirements, Design Reviews, and other topics as deemed necessary.



A System Safety Plan

- Encompasses the payload project's complete system safety program consistent with NPR 8715.3 and shall include:
- *Note: MIL-STD-882, Department of Defense Standard Practice for System Safety also provides guidance for a system safety program.*
- A system safety roles and responsibilities section describing:
 - Interfaces and lines of communication with associated organizations including decision-making timelines and a description of the methods by which personnel may raise issues of concern to the project manager
 - Review and approval process (including identification of approving authorities) for commitment of assets to safety efforts
 - The staffing and responsibilities of key system safety personnel
 - The tasks and activities required to identify, evaluate, and eliminate or control hazards and to minimize risk



A System Safety Plan

- System Safety Program Milestones identifying and scheduling safety tasks and activities such as design analyses, tests and reviews and relating them to major project (mission) milestones
- System Safety Data identifying deliverable as well as non-deliverable data by title, number, date, and means of delivery or process for accessibility



A System Safety Plan (cont.)

- System Safety Interfaces identifying:
 - The interfaces between system safety and other applicable safety disciplines such as nuclear safety, facility or institutional safety, Range Safety, explosive and ordnance safety, chemical and biological safety, radiation safety, hazardous materials safety, fire safety, laser safety, software safety and any others
 - The interfaces between system safety and design systems engineering
 - The interfaces between system safety and other support disciplines such as maintainability, quality, reliability, software development, human factors engineering, industrial hygiene, and any others
 - The interface between system safety and all system integration and test disciplines



Preliminary Hazard Assessments and Hazard Reports

- The payload project shall utilize system safety engineering and analyses to identify and document potential hazards associated with the payload and verify how those hazards will be eliminated or controlled
- The preliminary hazard analyses presented at the time of the Payload Safety Introduction shall reflect the payload conceptual design, planned interfaces, operations, and identify potential hazards
- Hazard Reports shall identify the hazard, mechanism for occurrence and resulting outcome, worst case severity and probability, mitigations, and severity and probability with mitigations in-place
- Hazard Reports shall be included as part of each Safety Data Package



Safety Data Package I

- Descriptions of hazardous and safety critical flight hardware and software, systems, components and materials that comprise the payload and ground support equipment and reflect the PDR-level design and operations scenario of the payload
- A description of the payload and mission
- Initial descriptions of all payload systems including hazardous and safety critical subsystems, their operation and interfaces
- Preliminary hazard reports and summaries of the hazard analyses performed on payload systems
- Information identifying compliance to the Tailored Payload Safety Requirements
- For a project utilizing a previously-launched payload bus, identification and description of any payload safety related problems, mishaps, or failures that occurred during fabrication, testing, processing, or integration that could affect the safety of the flight hardware or software, ground support equipment, personnel or other NASA resources



Safety Data Package II

- Updated Safety Data Package I information that reflects the CDR-level design and operations scenario of the payload
- An updated description of the payload and mission scenario
- Updated Hazard Reports
- Detailed narrative descriptions of hazardous and safety critical subsystems, their operation and updated information identifying methods of compliance to the Tailored Payload Safety Requirements
- Detailed information of safety features, inhibits, monitoring systems, and their control and status during all processing phases (integration, test, pre-launch, launch, and return (if applicable))
- Supporting plans, studies, and reports shall be provided or referenced, and furnished upon request
- A description of the ground support equipment, summary of hazardous, non-hazardous, and safety critical operations, a list of hazard reports, and supporting hazard analyses for operations performed in NASA facilities, NASA contracted facilities, and at launch site facilities
- A cross-reference identifying the disposition of PSWG & Agency Team review comments of Safety Data Package I and indication of changes made



Safety Data Package III

- Includes all the Safety Data Package updates and address all comments, incorporate all changes that reflect the as-built configuration and planned processing activities
- The final as-built description of the payload and mission scenario
- Final Hazard Reports
- Updated descriptions of hazardous and safety critical subsystems
- Updates to supporting plans, studies, and reports; required summaries of test results shall be provided and furnished upon request
- A record of test failures, anomalies, and mishaps involving qualification hardware, flight hardware, ground support equipment, and software (if used for hazard control), and an assessment of the resolution and safety implications of these events
- A signed copy of approved safety waivers (with attachments provided upon request)
- A cross-reference identifying the disposition of review comments since the last Safety Data Package submittal and indication of changes made



A Safety Review III Presentation

- Summary of safety activities and reviews with dates and an update on the status of open safety related work
- Overview of safety non-compliances, risks and issues.
This shall include:
 - A synopsis of any waivers
 - Characterization of significant residual safety risks including their likelihood and associated consequences



Questions?

DRAFT ELV Payload Safety Review Process

Payload Organization

Agency Team

